20. (Amended) The method of claim 1, further comprising the step of:

receiving an authorization key from the [requester] second party.

21. (Amended) The method of claim 1, further comprising the step of:

authenticating the [requester] second party.

22. (Twice Amended) The method of claim 1, wherein the step of receiving a request message from the [requester] second party comprises the step of:

receiving a query for the first party's personal information in a readily executable form.

REMARKS

Applicants have carefully reviewed the office action dated August 7, 2002. This response is believed to address all grounds for rejection stated in the office action and to place the application in a condition for allowance.

Request for Continued Examination

Applicants hereby file an RCE to and request further examination of the finally rejected application. Appropriate fee is enclosed.

Amendments to the claims

Claims 1, 20-22 are amended to overcome the rejections stated in the office action. Claim 25 is now canceled and added to the co-pending continuation in part application. Therefore it is not addressed in this response. Reconsideration is requested.

Rejection of claims based on Section 102(e) in view of Ho

The Office action rejected all claims based on a newly discovered patent, USP 6,148,342 A, which was issued to Ho. Applicants respectfully traverse this rejection because (a) the invention date of the claimed invention was made

earlier than the filing date of the Ho patent, and (b) Ho does not anticipate the instantly claimed invention. Applicants present affidavits regarding invention date at a later time and at present elect to respond to the second point mentioned. Further, Applicants respond to Ho only with respect to the independent claims and prove that Ho does not anticipate the independent claims. And it is well understood that if the independent claims are allowable, then claims that depend on allowable independent claims are also allowable.

Ho is directed toward the following.

> "A receiving terminal receives a request for data from a user and encrypts an identifier with a first code and a data access request with a second code. The identifier and data access request are transmitted to a first database which decodes the identifier and determines whether the user has authorization to request the desired information. The first database then retrieves an associated access level and internal identifier. The first database forwards the still encrypted data access request with the associated access level and internal identifier to a second database. ¶ The second database retrieves the information requested in the data access request and in one embodiment, if the user has an appropriate access level, transmits the requested information to the receiving terminal." See Summary of the Invention.

Ho describes the following, which appears to have been the Examiner's reason to cite Ho as 102(e) art against the instantly rejected claims.

> The identifier database encrypts the internal ID, the privilege level, and the source terminal address in block 240 for transmission to a data request database in a separately administered subnetwork. The actual patient name as well as the doctor name is stripped from the data, identified only by an internal ID. In one embodiment of the invention, identifier database encrypts the internal ID with the public key of the data request database. In block 244 of FIG. 2B, the

data packet including the internal identifier, user access level or privilege level, along with the original encrypted data access request, is transmitted to the data request database in block 244. In one embodiment, an entry is added to a log to document the transmission in block 244. The transmission may be through a dedicated line or virtual private network to ensure data security and integrity. In one embodiment, the entire packet is encrypted and signed.

In block 248, the data request database decrypts the information received from the identifier database. In block 252, the data request database retrieves the patient's medical records file corresponding to the internal identifier. In decision block 256, the data request database determines if access to the particular information in the file is allowed based on the access privilege level received. If access is not allowed, a notice is sent to the source terminal in block 260.

When the privilege level authorizes access to the specific information, the data request database performs the requested operation and encrypts the result set in a data packet for transmission to the source terminal. In one embodiment, the requested information is encrypted with the public key of the source terminal in block 264. The public key of the source terminal could have been received with the data access request. The encrypted data is then transmitted back to the source terminal in block 268. The source terminal decodes the data and displays it to the authorized user.

By dividing the data in a transaction request packet into several parts, each part accessible to only one computer system or corresponding subnetwork run by corresponding independent system administrators, subject confidentiality and data integrity of the information is preserved. Each database, such as identifier 128 and data request database 152 can be implemented on standard computer systems. These systems may be integrated using a network of direct connections or if data

> transmissions are encrypted, using publicly available Internet connections.
>
> The previous descriptions also show the data flow flowing from a source terminal 104 to an identifier database 128 through the data request database 152 back to the source terminal. FIGS. 3A and 3B illustrate this basic structure without and with the log monitor, respectively. However, the invention should not be limited to such a data flow as other data flows are possible. FIGS. 3C and 3D illustrate alternative embodiments of information flow and data management system design. See Col. 6, l. 38 - Col. 7, l. 24.

What Ho teaches is evident from Ho itself. It is, though, clear that Ho does not disclose or teach the claimed step of "assigning at least one of a plurality of security levels to each information object at any granularity." See claim 1 and other independent claims. Nowhere does Ho teach or suggest assigning a security level to an information object. Nowhere does Ho teach or suggest that at different granularity, fine, coarse or medium etc., information objects can have security levels associated with them thereby allowing selective disbursement of personal information.

Because Ho does not teach or suggest this claimed step, Applicants respectfully traverse the rejection based on Ho. Reconsideration is requested. Applicants request the Examiner to grant an interview should there be a need for additional explanation.

Rejection of claims based on §103 in view of Ho and other references

The Office action rejected all claims based on Ho in combination with other previously cited art. Applicants hereby incorporate by reference all the arguments presented above with reference to Section 102(e) rejections and further argue that in view that the independent claims are believed to be patentable, the dependent claims are also believed to be patentable. Accordingly, Applicants respectfully request reconsideration.

Conclusion

Applicants have addressed all grounds for rejection as stated in the Office Action. In view of the aforementioned changes and remarks, Applicants believe that all currently pending claims in the instant are in a condition for allowance. Reconsideration and an early notice of allowance are respectfully solicited.

Respectfully Submitted,

(44,602)

Naren Chaganti
345 Sheridan Avenue, Suite 308
Palo Alto, CA 94306
(650) 248-7011 phone
(650) 838-0586 fax
naren@chaganti.com
Attorney for Applicants

Certificate of Mailing

I certify that this paper (together with any other papers mentioned or referenced herein as being enclosed) is mailed via First Class Mail to Assistant Commissioner for Patents, Washington, D.C. 20231.

February 24, 2003
Date

NAREN CHAGANTI